Program Cyber Security Plan

Exhibit 2 - Designated Approving Authority (DAA) Overview

1.0 Introduction

This overview describes the statutory authority, qualifications, and responsibilities of a Designated Approving Authority (DAA). The DAA is the senior government official who has the authority to decide on accepting the security safeguards prescribed for the Office of Science's (SC) information systems. Every information system in SC must have an Authority to Operate (ATO) in order to be on the network and operational. By signing the ATO for a system, the DAA is accepting responsibility for the level of risk inherent in that system.

Statutory authority for a DAA responsibility stems from the Federal Information Security Management Act (FISMA). § 3544 describes Federal Agency responsibilities and states:

> ‘‘(a) IN GENERAL.—The head of each agency shall—
> (2) ensure that senior agency {Federal} officials . . .
> (A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;”

Further, FISMA requires the implementation of National Institute of Standards and Technology (NIST) Standards. NIST Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires the implementation of NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, which states:

> “The *authorizing official* (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.”

The Office of Science through the DAA will adhere to the NIST Certification and Accreditation guidance as set forth in Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

2.0 Qualifications

The DAA is the senior government official with the authority to assume formal responsibility for operating a system at an acceptable level of risk, based on the implementation of an approved set of technical, managerial and procedural safeguards. The DAA must be at an organizational level such that he or she has authority to evaluate the overall mission requirements of SC and to provide definitive directions to SC system developers or system owners relative to the risk in the security posture. Therefore, the DAA must:

- Be a senior level employee of the United States Government;
- Hold United States Government security clearances/access approvals corresponding with the level of information processed by the system; and
- Understand the operational need for the system(s) in question and the operational consequences of not operating the system(s).

In Office of Science, the DAAs are the Federal Integrated Service Center or Site Office managers.

3.0 Responsibilities

The DAA’s responsibilities include the following:

- Ensures that each information system under his or her purview has completed the C&A process including adherence to the guidelines as set forth by NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* and has all supporting system documentation.
- Understands and accepts the residual security risk for the information systems and networks on behalf of SC. The **residual security risk** is the amount of risk that remains after all controls have been implemented and mitigation efforts have been completed. It is important for the DAA to understand that risks cannot be completely eliminated. It is the responsibility of the DAA to determine if the amount of residual risks that remain after all security measures have been taken is acceptable for his or her information system. Based on the residual risk level, the DAA may approve, suspend, or terminate operation of information systems under his or her purview in accordance with National and Departmental policy. The Department of Energy (DOE) only accepts ATO or Denial of ATO.
- Ensures that personnel performing cyber security responsibilities are properly trained.
- Directs line management assessment and monitoring of the cyber security program at the site for which they are responsible.
- Ensures that documentation is maintained for all information system accreditations under the DAA’s purview.

- Ensures that personnel are performing their cyber security responsibilities in accordance with the Department's directives and SC direction on each information system.

- Ensures that security is incorporated as an element of the system lifecycle process.

- Approves the classification level that is required for applications to be implemented in a network environment. In addition, approves security services that are necessary (e.g., encryption and non-repudiation) to interconnect to external systems.

4.0 Accreditation and Certification Process

FISMA, NIST, Departmental policy, and SC policy requires the Office of Science to perform the C&A process on each of its information systems. This process must be completed either every 3 years or when there is a significant change that affects the system's security posture. This includes all major applications and general support systems.

The purpose of the C&A process is to ensure that information systems have adequate security commensurate with the level of risk. To this end, the C&A is the formalized process used to assess the risks and security requirements for each system, and to determine whether the system's security needs are being met.

The DAA will assist in the implementation of a certification program to test and evaluate technical and non-technical IT security features and other safeguards used by the Office of Science (SC), in support of the C&A process. The process will not only address software and hardware security safeguards, but also procedures, physical protections, and personnel security measures.

The following minimum requirements must be met for a system to be certified:

- The system must be thoroughly documented.
- A system security plan must be developed and approved.
- A Security Testing and Evaluation (ST&E) of the system must be completed.
- A risk assessment must be conducted.
- Standard operating procedures must be developed for the system.
- A contingency plan must exist for the system.

5.0 Authority to Operate (ATO)

The Authority to Operate (ATO) is the formal declaration from the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards. ATO's must be renewed at least every three years or when there is a significant change to the system. It contains a statement from the DAA that the system has the authority to operate with the controls and processes that are in place or will be implemented per the Plan of Action and Milestones (POA&M).

The contents of the ATO package are all the analysis and documentation describing the environment of the systems, roles and responsibilities of the key personnel, and description of the controls in place.

Since the premise of the cyber security program is the implementation of cost effective security control, some vulnerabilities will not be mitigated because the cost of mitigation exceeds the benefit realized. The risk assessment is the acknowledgement that not all vulnerabilities have been corrected; however, the residual risks have been reduced to a level sufficient to protect the information being processed, transmitted or stored.

6.0 Important Terms

Authority to Operate (ATO) – A letter signed by the DAA formally allowing a site or laboratory to operate their information systems. An ATO may be for a defined term or it may be issued for up to three (3) years. ATOs may have conditions, e.g., a laboratory may have to meet commitments in its Plan of Action and Milestones per and agreed upon timeline.

Certification and Accreditation (C&A) Package - The required set of documentation for an information system that is necessary for an ATO approval.

Designated Accrediting Authority (DAA) - The government official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. The term "designated accrediting authority" and "delegated accrediting authority" is synonymous

Management Controls - The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Operational Controls - The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Policy - The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system.

Procedure - The steps contained in a policy that are necessary for compliance.

Residual Risk - The portion of risk that remains after security measures have been applied.

Risk Management - The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Risk Mitigation - The process of removing or reducing risk. Risk mitigation may include risk analysis, or other activities designed to assess the results of risk mitigation initiatives.

Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Testing and Evaluation (ST&E) - The process that examines or analyzes the protective measures that are placed on an information system once it is fully integrated and operational.

System Security Plan - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Technical Controls - The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

7.0 Reference Documents

Circular No. A-130, *Revised, Management of Federal Information Resources*

DOE P 205.1, *Departmental Cyber Security Management Policy*

DOE O 205.1, *Department of Energy Cyber Security Management Program*

DOE O 470.1, *Safeguards and Security Program*

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

NIST SP 800-37, *Guidelines for Security Certification and Accreditation of IT Systems*

NIST SP 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*